Advisory 2018-10

Security update for CODESYS Control V3 security features

Published: 19 December 2018

Version: 3.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2018-10_CDS-61037.docx

© 3S-Smart Software Solutions GmbH

CONTENT

Template: templ_tecdoc_en_V2.0.docx

© 3S-Smart Software Solutions GmbH

1 Affected Products

All variants of the following CODESYS V3 products in all versions prior V3.5.14.0 containing the CmpSecureChannel or CmpUserMgr component are affected, regardless of the CPU type or operating system:
• CODESYS Control for BeagleBone
• CODESYS Control for emPC-A/iMX6
• CODESYS Control for IOT2000
• CODESYS Control for Linux
• CODESYS Control for PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control RTE V3
• CODESYS Control RTE V3 (for Beckhoff CX)
• CODESYS Control Win V3 (also part of the CODESYS setup)
• CODESYS V3 Simulation Runtime (part of the CODESYS Development System)
• CODESYS Control V3 Runtime System Toolkit
• CODESYS HMI V3

2 Vulnerability overview

2.1 Type

Access control inactive by default

2.2 Management Summary

Currently neither communication encryption nor user authentication is activated by default, but must be activated by the user.

2.3 References

CVE: CVE-2018-10612 [6]

ICS-CERT: ICSA-18-352-03 [8]

CODESYS JIRA: CDS-61037

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as critical.

The CVSS v3.0 base score of 9.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. The CODESYS Control runtime system provides several security features. To limit the access to the programming port, it allows defining users with individual passwords or also to configure a role based user management with graded access rights and multiple users. To protect the user credentials on the line, the communication can optionally be encrypted by a TLS based protocol. Currently neither encryption nor user authentication is activated by default or can be enforced by the user.

3.2 Exploitability

This vulnerability could be exploited remotely.

Template: templ_tecdoc_en_V2.0.docx

© 3S-Smart Software Solutions GmbH

3.3 Difficulty

An attacker with low skills would be able to exploit a PLC without activated user management and/or communication encryption.

3.4 Existence of exploit

No known public exploits specifically target this vulnerability.

4 Available software updates

This issue is solved in two steps to allow communication clients beside the CODESYS Development system to find a compatible update strategy.

With the already released version V3.5.14.0 of the affected products, the CODESYS development system V3.5.14.0 enables the configuration of the communication and the user management policy of the affected products in online mode by the CODESYS development system. In the communication settings dialog of the CODESYS development system, where the path to the PLC is configured, there is a clearly visible link to the CODESYS online help to explain the technical background and to remind the user to activate these features. This allows customers to activate and enforce communication encryption and user management.

In the second step, it is planned to activate both features by default with version V3.5.15.0 of the affected products.

The release of version V3.5.15.0 is expected for July 2019.

Please visit the CODESYS update area for more information on how to obtain the software update [3].

5 Mitigation

The encryption of the online communication and the online user management of CODESYS control runtime systems is already available since several service packs of the affected products. Depending on the PLC runtime system, these features can be activated by the user or only by the control manufacturer. Further information on how to activate encrypted communication and user management can be found in the CODESYS online help.

In general, 3S-Smart Software Solutions GmbH recommends as part of the mitigation strategy the following defensive measures to reduce the risk of exploitation of this vulnerability:

- Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
- Use firewalls to protect and separate the control system network from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control system by using up to date virus detecting solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

6 Acknowledgments

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

We thank Yury Serdyuk of Kaspersky Lab for reporting this vulnerability following coordinated disclosure.

Template: templ_tecdoc_en_V2.0.docx

© 3S-Smart Software Solutions GmbH

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

3S-Smart Software Solutions GmbH assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided on good faith by 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

Template: templ_tecdoc_en_V2.0.docx

© 3S-Smart Software Solutions GmbH

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH CODESYS update area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/fileadmin/data/customers/security/2018/Advisory2018-10_CDS-61037.pdf

Change History

Version	Description	Date
1.0	First version	06.12.2018
2.0	Software update available	17.12.2018
3.0	Reference to ICS-CERT advisory added	19.12.2018

Template: templ_tecdoc_en_V2.0.docx

© 3S-Smart Software Solutions GmbH